

REMARKS

Applicants request favorable reconsideration and allowance of the present application in view of the foregoing amendments and the following remarks.

Claims 38-42, 45-50, 53-58, 61-66, and 69-73 are pending in the present application. Claims 38-41 are the independent claims. Claims 43, 44, 51, 52, 59, 60, 67, and 68 have been cancelled without prejudice.

Claims 38-41 have been amended. Applicants submit that support for these amendments can be found in the original disclosure at least, for example, at page 12, lines 5-7 of the specification. Therefore, no new matter has been added.

Applicants appreciate the courtesies extended by Examiner Ho in granting and conducting a personal interview with Applicants' representative on November 15, 2005.

Below is a summary of the discussion at that interview.

All pending claims were rejected as being either anticipated or obvious over Friedman. Applicants respectfully traverse these rejections for the reasons discussed at the interview and presented below.

As discussed at the interview, and as discussed in the background section of the specification, the prior art includes a system for confirming authenticity of a message where unique data corresponding to the message is generated (for example, by using a hash function), and a private key is used to encrypt the unique data. The encrypted data is transmitted with the message. At the receiving side, a public key is used to decrypt the unique data. The same procedure for generating the unique data, e.g., a hash function, is applied to the received message. If the unique data generated from the received message matches the decrypted unique data generated from the message at the transmitting side, the

authenticity of the received message is confirmed. Thus, the prior art system first generates unique data, then performs encryption using confidential information (i.e., a private key) to permit authentication. However, since private key/public key encryption and decryption requires complex mathematical operations, it requires significant processing capabilities and time.

As recited in independent Claim 38, for example, the present invention includes, *inter alia*, the features of performing a predetermined calculation unit using an encoded digital image and confidential information, and then generating additional data using a result of the predetermined calculation. With these features, authentication can be performed but it is unnecessary to perform private key/public key encryption and decryption. Therefore, processing power and time can be saved.

Applicants submit that Friedman discloses a system just like the background prior art. In particular, Friedman discloses that an image is first hashed to generate unique data, and then a private key is used to encrypt the result of the hash function. See, e.g., col. 4, lines 34-36 and 44-45. Thus, Applicant submits that the invention of Claim 38 uses confidential information as an argument in a predetermined calculation in a first step, whereas Friedman discloses using confidential information (i.e., a private key) in a second step *after* a hash function is performed. Accordingly, that patent fails to disclose or suggest at least the claimed features of Claim 38 of performing a predetermined calculation using an encoded digital image and confidential information, and then generating additional data using the result of the predetermined calculation.

The Office Action asserted that, because additional data can be recorded in the border of an image, the hash and encryption of that border information forms only part of a

digital signature and there is additional using of that result to form the final digital signature. Applicants respectfully disagree. Friedman discloses that the information recorded in the border area is hashed and encrypted *together with* the image (see col. 4, lines 63-66). Thus, it is the hash and encryption of the combined image and additional data that collectively forms the digital signature, and no further step is required.

For the foregoing reasons, Applicants submit that Claim 38 is patentable over Friedman. Independent Claims 39-41 include similar features and are believed patentable for similar reasons.

During the interview, the Examiner referred to other systems that he believed to be prior art that use multiple encryption, such as Triple DES. The Examiner asserted that the pending claims would read on such a system because the predetermined calculation would read on the first encryption pass and the generation of additional data using the result of the predetermined calculation would read on the second encryption pass.

Without conceding that Triple DES or any other multiple encryption system is in fact prior art, Applicants have amended independent Claims 38-41 to recite that the generation of additional data uses the result of the predetermined calculation and a one-way function. Since encryption does not use a one-way function (the encrypted data must be capable of being decrypted), Applicants submit that Claims 38-41 would not be unpatentable over a multiple-encryption system as described by the Examiner during the interview.

Accordingly, Applicants submit that the prior art of record does not disclose or suggest at least the features of performing a predetermined calculation using an encoded digital image and confidential information and then generating additional data using the

result of the predetermined calculation and a one-way function, and therefore Claims 38-41 are patentable.

The dependent claims are believed patentable for at least the same reasons as the independent claims, as well as for the additional features they recite.

For the foregoing reasons, this application is believed to be in condition for allowance. Favorable reconsideration, withdrawal of the outstanding rejections, entry of this Amendment, and an early Notice of Allowance are requested.

Applicants' undersigned attorney may be reached in our Washington, DC office by telephone at (202) 530-1010. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,



Attorney for Applicants
Brian L. Klock
Registration No.36,570

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200
BLK/lmj
DC 171859v1